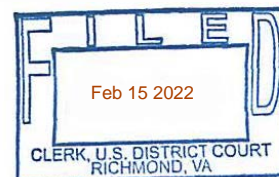


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
M.ATIF.AKHTAR@GMAIL.COM AND
AKHTARMA@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE, LLC

Case No. 3:22sw31

Filed Under Seal



**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Deputy United States Marshal (DUSM) Andrew Recker, being first duly sworn, hereby
depose and state as follows:

I. INTRODUCTION

A. Purpose of Affidavit

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), an electronic communications service provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The accounts to be searched are: (1) M.atif.akhtar@gmail.com (hereinafter, "TARGET ACCOUNT 1"); and (2) akhtarma@gmail.com (hereinafter, "TARGET ACCOUNT 2") (collectively, the "TARGET ACCOUNTS"), which are further described in the following paragraphs and in Attachments A-1 and A-2, respectively. The information to be searched, disclosed, and seized is described in the following paragraphs and in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the

government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe the TARGET ACCOUNTS contain evidence of and were used in connection with a violation of 18 U.S.C. § 2261A(2)(B) (Stalking). There is also probable cause to search the information described in Attachment A-1 and A-2 for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B. Specifically, there is probable cause to believe that this email account was used to send and/or deliver threatening communications to specific government officials. In executing such a search warrant, your affiant expects to find records that identify the owner of the email account to include IP information, geolocation, addresses, phone numbers, payment information, linked accounts and/or devices, possible additional evidence related to threatening communications, and potential evidence of additional crimes or victims.

B. Agent Background and Experience

4. As a DUSM, I am a Criminal Investigator with the United States Marshals Service (USMS) and have been so employed for over 11 years. I am a graduate of the Federal Law Enforcement Training Center (FLETC) and the USMS Basic Training Academy. As a Criminal Investigator with the USMS, I am a federal law enforcement officer of the United States within the meaning of 18 U.S.C § 3053 and 28 U.S.C. § 566. As outlined in these statutes, I am authorized to investigate offenses against the United States, and I am further authorized to conduct arrests when I have reasonable grounds to believe the person has committed or is committing a felony. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This

affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. I served as a DUSM in the District of Columbia prior to my current assignment as the Protective Intelligence Coordinator (PIC) within the Judicial Security Unit (JSU) for the USMS – Eastern District of Virginia (EDVA). In this capacity, I support USMS missions to ensure the safety and security of the federal judiciary, the judicial process and its participants. As defined under 28 U.S.C. § 566(e)(1)(A), the USMS has the statutory authority to conduct investigations relating to threatened persons in the interest of justice and where criminal intimidation impedes the judicial process. I received specialized training on threat investigations and a multitude of federal offenses, to include search and seizure and arrest laws, at the Protective Intelligence Training Course (PITC) offered by USMS Headquarters, where I also serve as an instructor for Protective Intelligence Investigators (PIIs) and District Threat Investigators (DTIs) within the USMS. I regularly refer to my USMS and partner agency training during the course of my official duties.

6. During my career with the USMS, to include through my involvement in task forces, I have handled informants, investigated complex criminal violations, and located and arrested fugitives for a variety of crimes, to include failure to register as a sex offender (Adam Walsh Act), amongst others. I have also been the affiant on numerous search warrants associated with locating fugitives and to obtain evidence, to include electronic evidence. In turn, I have also been involved in the execution of search warrants, to include warrants authorizing the search and seizure of physical evidence, e.g., from residences, and those requiring service on telecommunications or internet service providers for stored and/or real-time electronic information, records, and data.

7. I am also a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force. Pursuant to my position as a TFO, I have investigated several complex terrorism cases, some of which resulted in federal prosecution.

8. The information contained in this affidavit is based upon my personal investigation, my review of the reports and files in this case, conversations with other law enforcement personnel, and other information sources that I believe to be reliable. I have collaborated with USMS personnel in the EDVA, USMS Headquarters, as well as partner agencies, in furtherance of this investigation. The following is not an exhaustive enumeration of the facts I have learned during the course of the investigation. Instead, they are the facts which I believe support a finding of probable cause for the requested warrant and does not set forth all of my knowledge about this matter. To the extent that conversations or interviews of witnesses and/or subjects are described herein, the statements are provided in summary fashion unless otherwise noted with direct quotations. Further, my understanding of the facts and evidence as presented in this Affidavit may change or evolve as the investigation progresses and new information is learned.

C. Suspected Criminal Violation

9. Title 18, United States Code, Section 2261A(2)(B) (Stalking) prohibits, in pertinent part, a person from traveling in interstate or foreign commerce, with the intent to kill, injure, harass, intimidate, or place a person under surveillance. This statute further prohibits the use of mail, any interactive computer service, or electronic communication service, or use of any other facility affecting interstate commerce to engage in this course of conduct. These actions may cause, attempt to cause, or reasonably be expected to cause, substantial emotional distress for the person being placed under such surveillance.

II. LEGAL AUTHORITY

10. The legal authority for this search warrant application regarding the Google accounts is derived from 18 U.S.C. §§ 2701-2711, entitled “Stored Wire and Electronic Communications and Transactional Records Access.” Section 2703(a) provides, in relevant part, as follows:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C. § 2703(b) provides, in relevant part, as follows:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the

provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

11. The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

III. JURISDICTION

12. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction,” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated herein, because the subscriber of the subject email address and person suspected to be responsible for the threatening interstate communications resides in Henrico, Virginia.

IV. BACKGROUND CONCERNING GOOGLE ACCOUNTS

13. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain gmail.com, like the email accounts listed in Attachments A-1 and A-2 (i.e., the TARGET ACCOUNTS). Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide

basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

15. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. Based on my training and experience, I am aware that in addition to email, Google accounts contain a variety of data and services including but not limited to the following:

17. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;

- a. Google maintains information about its customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers;

18. Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) of all associated devices linked to the Google accounts of the target device.

- a. Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s);

19. User attribution data - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);

- a. I know that Google may not verify the true identity of an account creator, account user or any other person who accesses a user's account using login credentials. For these reasons, it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data, usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons, it may be necessary to search and analyze data from when the Google account was initially created to the most current activity;

20. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;

- a. Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and

remains so unless the user adds a third-party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. I believe this information will identify dates and appointments relevant to this investigation, as well as to identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence;

21. Contacts - All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
 - a. When a user links the Android device to their Google account the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process is continuously updates so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. I believe this information is pertinent to the investigation as it will assist with identifying previously unknown coconspirators and/or witnesses.
22. Documents - All user created documents stored by Google;
 - a. Google offers users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. I believe this information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales, communications with

unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation;

23. Gmail - All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;

- a. As noted previously, when user of an Android device first activates the device they are prompted to associate the device with a Google mail, commonly referred to as Gmail, account.
- b. The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account, they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Gmail are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. I believe these messages would reveal motivations, plans and intentions, associates, and other co-conspirators;

24. Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;

- a. Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. I believe a review of these images would provide evidence depicting the suspect, his/her associates and others performing incriminating acts, and victims. I also believe these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation;

25. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings for the period specified in Attachment B;

- a. Google collects and retains location data from Android enabled mobile devices. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. I believe this data will show the movements of the suspect's mobile device and assist investigators with

establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation;

26. Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;
 - a. Google operates an online marketplace whereby Google and other third-party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi.
 - b. These various applications facilitate communication via voice using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media message system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service network there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants. Furthermore, identifying the user's applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications would assist locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous appearing program, but are used to

conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal;

27. Google Hangouts – A Google application which allows Google accounts to communicate with other Google accounts.

- a. Google Hangouts enables users to communicate through video calls, voice calls, and one-on-one or group messaging. Additionally, users can send and receive files as attachments, such as photos or maps. I believe these messages would reveal motivations, plans and intentions, associates and other co-conspirators.

28. Search History - All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;

- a. Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user selected results. Furthermore, these searches are differentiated by the specific type of search a user performed into categories. These categories include a general web search, and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping.
- b. I believe a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it;

29. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device;

- a. Google offers users access to a free voice over internet protocol (VOIP) communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user's actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages. The service also has a voicemail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as, any saved voicemail messages and the associated transcriptions;

30. Wallet/Checkout - All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book;

- a. Google operates a financial services division that allows users to make online purchases through Google and other vendors, as well as, send and receive money from other users. Applications that are purchased and installed on a mobile device are handled by Google's Wallet/Checkout service. The purchase and installation of

applications on a mobile device requires the use of the Google Wallet service. Therefore, any applications installed on the suspect's mobile phone have a transaction record in Google Wallet. Google stores information regarding the transactions including the date and time of the purchase. Additionally, they have method of payment information such as associated credit card numbers used to facilitate the purchase. Other data includes the billing address of any linked credit card and any addresses where purchased products were shipped to. I believe identifying the method of payment information would assist investigators with identifying any previously unknown financial institutions and that these financial institutions may have additional relevant information pertinent to this investigation.

31. Google Home (Smart Speaker & Home Assistant) - All information related to Google Home including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times;

- a. Google Home is a brand of smart speaker developed by Google, LLC. Google Home Speakers have microphones that are always listening that enable users to speak voice commands to interact with services through Google's intelligent personal assistant called Google Assistant. A large number of services, both in-house and third-party, are integrated, allowing users to listen to music, control playback of videos and photos, and receive news updates entirely by voice. Google Home devices also have integrated support for home automation, letting users control smart home appliances with their voice. Multiple Google Home devices can be placed in different rooms in a home for synchronized connectivity. The data collected by Google Home devices are stored remotely on Google's servers. Users

can access their Google Home account and associated data by way of a connected smart phone application or through their Google account. I believe the Google Home related data, including the archived audio recordings may be used to refute and corroborate statements, and may be important in identifying potential witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing a timeline and provide context and intent.

32. Android Auto - All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and all location data;

- a. Android Auto is a mobile device application developed by Google that allows enhanced use of an Android device within a vehicle equipped with a compatible head unit. Once the Android device is connected to the head unit, the system enables it to broadcast applications (apps) with a simple, driver-friendly user interface onto the vehicle's dash display, including GPS mapping/navigation, music playback, text messages (SMS), voice calls, and web search. The system supports both touchscreen and button-controlled head unit displays, although hands-free operation through voice commands is encouraged. Once the user's Android device is connected to the vehicle, the Android mobile device will have access to several of the vehicle's sensors and inputs, such as GPS, steering-wheel mounted buttons, the sound system, directional microphones, wheel speed, compass, and other vehicle data.
- b. I believe the Android Auto related data, including the historical geo-location data (GPS, compass, speed, direction) may be important in establishing locations and

activities of possible witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing the driver and occupants of a particular vehicle, refute and corroborate statements, and can be used to establish a timeline and provide context and intent.

33. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation.

For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

34. According to Google's Privacy & Terms web site (found at the following location: <https://www.google.com/policies/technologies/cookies>), the company sends a small piece of text (known as a "cookie") to the user's internet browser for a variety of purposes. Cookies allow the web sites visited, such as Google.com or Gmail.com, to recognize the electronic device that is accessing that web site. Google's cookies record: (a) all of the Google accounts accessed by a particular electronic device using the same web browser; (b) information about those visits; and (c) the user's preferences and other settings. When that device returns to the web site later, Google can then tailor the user's online experience accordingly. Through the use of these cookies, Google is able to establish a relationship between multiple Google accounts that are likely used by the same individual.

V. PROBABLE CAUSE

A. Overview of Investigation

35. The United States, including the United States Marshals Service (USMS), is conducting a criminal investigation of MOHAMMAD ATIF AKHTAR, as well as identified, and as any yet unidentified, subjects regarding possible violations of 18 U.S.C. § 2261A (Stalking). The investigation arises from AKHTAR's repeated efforts to contact a Department of Justice employee (herein, the "VICTIM") working at the U.S. Attorney's Office (USAO) in the Eastern District of Virginia (EDVA). AKHTAR initially communicated with VICTIM when he walked into the USAO with a purported criminal complaint. AKHTAR then persistently made efforts to call, email, and visit VICTIM in-person at her work. Later, AKHTAR reached out to VICTIM

via VICTIM's personal social media account and sent flowers to her home address. As detailed below, this Affidavit is submitted in support of a request for authority to obtain information and data from AKTAR's Google accounts.

B. Timeline of AKHTAR's Contact and Efforts to Connect with VICTIM in 2020

36. In April of 2019, VICTIM, an Assistant United States Attorney (AUSA), was on duty at the EDVA USAO in Richmond, Virginia. (AUSAs are on duty on a rotational basis and, as part of this role, they assist with walk-in citizen complaints, covering certain court appearances, and handle other matters.) In his/her role as the duty AUSA, VICTIM had his/her first interaction with AKHTAR when walked into the USAO in Richmond. VICTIM met with AKTHAR and he reported wanting to file a complaint regarding racial profiling at a Department of Defense (DOD) facility where he worked. VICTIM stated s/he directed AKHTAR to contact the Federal Bureau of Investigation (FBI) to file a report. This is a commonplace referral, as law enforcement agencies, such as the FBI, typically conduct assessments on whether to open investigations on claimed criminal misconduct.

37. After this initial contact, AKHTAR returned to the USAO several times, and each time VICTIM stated s/he directed the receptionist to tell AKHTAR s/he could not meet with him. VICTIM stated since that time AKHTAR continued to call and send emails, which were not responded to due to the above-stated referral to the FBI.

38. On or about September 9, 2020, VICTIM received a series of inappropriate communications from AKTAR that were voluminous and solicitous, but not overtly threatening in

nature based on content alone.¹ VICTIM described a series of inappropriate communications s/he received from Mohammad Atif AKHTAR, including several emails, phone calls, and one voice message. VICTIM also noted that AKHTAR attempted to make internet contact on Facebook and Instagram by sending instant messages, voice calls, and video calls on the platform messaging programs. VICTIM stated s/he never replied to any of these communications, and that privacy settings prevented AKHTAR from making contact through social media accounts.

39. In fact, VICTIM reported that s/he only became aware of AKHTAR's attempts to contact him/her when VICTIM switched the Facebook and Instagram privacy settings "to make a particular post public." VICTIM stated that after submitting the public post, s/he returned the settings to "private," and thought no more of it. However, s/he became concerned when a voicemail and email from AKHTAR were received on or about [REDACTED]. The email concluded with a post-script which read, "P.S. Happy Birthday! Hope you have an amazing day full of stress-free living and be internally joyful!"

40. As investigators, AKHTAR's repeated efforts to contact VICTIM and conduct social media research to learn more information him/her via personal social media profiles is of particular concern to USMS investigators. In stalking cases, I know from training and experience

¹ Based on my training and experience, I know that individuals engaged in stalking-type behavior may not necessarily send messages that are individually threatening. Instead, an individual's suspected involvement in such criminal conduct can sometimes be initially detected based on the collective content and frequency of the messages or communications sent from the suspect to the victim. In some instances, the volume of messages are indicative of a potentially dangerous obsession with a victim and/or the content of the messages can reveal a misdirected, inaccurate presumed closeness to the victim extending beyond the objective nature of the relationship.

In this case, I have had the opportunity to review reports regarding the communications and, in other instances, the messages themselves. Based on my review, as detailed in subsequent sections of this Affidavit, I observed both types of concerning indicators in terms of volume and collective content.

that perpetrators can develop a fascination with their victims, which can entail seeking to learn personal details of the victims' lives such as their birthday.

B. Investigators Contact AKHTAR in 2020

41. On or about September 22, 2020, DTI Moore and I met with AKHTAR at his home located at 3820 Redstone Drive, Richmond, Virginia. When DTI Moore and I arrived, AKHTAR was waiting outside in the driveway of his home. DTI Moore observed AKHTAR appeared neatly dressed and fairly well-groomed. However, despite his normal appearance, it was apparent AKHTAR was apprehensive and perhaps slightly paranoid.² For example, AKHTAR approached DTI Moore and asked her to fill out a "contact information and purpose of visit" form he had created before investigators began their interview. The form requested DTI Moore's phone number, work address, email address, name of immediate supervisor, supervisor's phone number, and an explanation of the purpose of their visit. AKHTAR stated that the form was "for [his] protection," and he started using it because he "has had false reports filed against [him] before."

42. I asked where AKHTAR would be more comfortable sitting down to talk, but he remained reluctant to go inside his home, suggesting they all sit on the back porch. AKHTAR stated that 3820 Redstone Drive was his "family home," and that his family had lived there "for a very long time." However, when asked if he lived alone, AKHTAR was evasive. DTI Moore informed AKHTAR that investigators were present to speak about some communications he sent to the USAO in Richmond, VA. In response, AKHTAR explained he was attempting to file a complaint regarding what he believed to be criminal activities he had observed while he was a

² From my training and experience, I know that individuals with mental health issues can become obsessed with others and/or imagine relationships. As such, the general mental state of AKHTAR is important to investigators. Through the course of the investigation, I received a report from one of his family members that AKHTAR is likely a paranoid schizophrenic.

contractor employed by DoD. AKHTAR stated that he had sent several emails and other messages to VICTIM just to make sure s/he was well informed about the status of the case he was trying to file.

43. In order to redirect AKHTAR's focus, DTI Moore explained that she wanted to clarify the investigative process with AKHTAR, to be sure he followed the appropriate steps as a complainant. DTI Moore and I explained to AKHTAR that it was not appropriate for AKHTAR to contact the USAO, VICTIM, or any other AUSA directly about his case. I explained that while AKHTAR initially spoke to VICTIM, s/he was not assigned to his case, and therefore would not be able to assist him. It was further explained to AKHTAR that he did not have a case pending with the USAO, because he did not follow the appropriate procedures. Investigators explained that the proper procedure for complainants is to contact a law enforcement agency and to allow that agency to conduct an investigation, and then to depend on the law enforcement agency to communicate with the USAO on behalf of the complainant. Investigators repeatedly asserted AKHTAR should have no further communications with VICTIM or any other AUSA. Further, that AKHTAR's attempts to contact any AUSA personally could be detrimental to his goal.

44. Though AKHTAR was lucid and attentive throughout the above-described conversation, AKHTAR often became distracted and circled back to repeat topics that had already been discussed. AKHTAR often mentioned he had cases pending with the Office of Special Counsel (OSC), and the Merit Systems Protection Board (MSPB), and that he had purportedly retained a lawyer to help him. AKHTAR also stated that in filing these complaints, he was acting as a whistleblower. Each time the conversation returned to AKHTAR's desire to file more information regarding his complaints, DTI Moore and I redirected the conversation back to the

assertion that AKHTAR should utilize his lawyer and contact a law enforcement agency, and that it was not appropriate, nor would it be useful, to contact the USAO or any AUSA.

45. By the end of the conversation, AKHTAR seemed to agree that contacting the USAO would not be helpful or appropriate. AKHTAR stated he did not previously have a good understanding of the process for filing criminal complaints, and he thanked DTI Moore and I for the help.

46. On or about October 29, 2020, DTI Moore and I closed the USMS's investigation into AKHTAR. AKHTAR did not attempt to contact the USAO or VICTIM since being interviewed by the USMS in September 2020. During this period, DTI Moore and I believed the efforts to redirect AKHTAR's focus away from VICTIM were successful.

C. Timeline of AKHTAR's Conduct in 2021 and Use of TARGET ACCOUNT 1

47. On or about October 14, 2021, VICTIM notified DTI Moore about new additional inappropriate communications that s/he received from Atif AKHTAR. USMS investigators were informed AKHTAR sent two emails on or about October 14, 2021 to VICTIM from email address: m.atif.akhtar@gmail.com (i.e. TARGET ACCOUNT 1). The subject of the first email was "Re: Atif Akhtar - Walk In: Racial Profiling Case" and the body of the email contained various messages from AKHTAR, some of which were AKHTAR's reports that referenced the Henrico Commonwealth Attorney's Office. AKHTAR concluded his email by saying, "Please let me know when I can come see you, I would love to. Thanks again! Atif Akhtar". The second email AKHTAR sent to VICTIM contained similar language of AKHTAR's desire to report crimes he felt were being committed against him that AKHTAR had attempted to report to the Henrico Commonwealth Attorney's Office.

48. On or about November 7, 2021, DTI Moore received a call from VICTIM.

VICTIM reported s/he had just returned home to find flowers delivered on his/her residence doorstep. The flowers were sent from a flower delivery service called "FromYouFlowers.com," and included a note which read: "Congrats [REDACTED] Barbie! - ... Ken."³ VICTIM stated s/he had called the flower delivery company to ask who had sent the flowers. The company advised they would have to reach out to the sender to get their permission to disclose the sender's identity. After a short time, the flower delivery company called back and informed VICTIM that the sender was Atif AKHTAR. Due to the USMS concern for the safety and security of VICTIM, USMS Investigators took steps to protect VICTIM's home, including requesting assistance from the police department.

49. Per VICTIM, s/he had never provided AKHTAR with information about his/her home address nor directly interacted with AKHTAR outside the summarized, above-described encounters at the USAO. The delivery of flowers to his/her home address caused fear and distress to VICTIM and VICTIM immediately went to stay at a friend's house. Since approximately November 7, 2021, VICTIM has not stayed at his/her own residence and believes remaining away from said residence is in the best interest of his/her safety and well-being. The change in VICTIM's residence has negatively impacted this prosecutor's personal and professional life.

///

///

³ The message is partially redacted to protect VICTIM's identity. The redacted reference identifies his/her position within the EDVA USAO at the time he/she received the flowers. Here, use of the names "Barbie" and "Ken" caused concern for investigators as the sender appears to imply that he and VICTIM are in a romantic relationship by using the names of boyfriend and girlfriend dolls created by Mattel.

D. AKHTAR'S Possession of a Firearm

50. Through this ongoing investigation, USMS Investigators discovered in May 2021 AKHTAR had his rights restored in the State of Virginia to purchase a firearm. Pursuant to that legal right, USMS investigators identified through the Virginia State Police that AKHTAR purchased a firearm, namely a shotgun, from a pawn shop in Richmond, Virginia on or about July 26, 2021. Further investigation revealed that AKHTAR later sold the firearm back to a pawn shop on or about November 20, 2021.

51. AKHTAR's criminal history consists of AKHTAR having a minimal criminal record with information reviewed consisting mostly of traffic violations, plus one felony conviction for grand larceny from 2001.

E. Additional Probable Cause Related to Use of the TARGET ACCOUNTS and Google Services

52. In January 2022, USMS Investigators served a subpoena to "From You Flowers, LLC" at 143 Mill Rock Road East, Old Saybrook, Connecticut 06475-4217. Pursuant to this subpoena, "From You Flowers" returned the detailed purchase information regarding the flowers that were delivered to the VICTIM's residence. On November 5, 2021, Atif AKHTAR, 3820 Redstone Drive Henrico, Virginia 23294, using the email address of akhtarma@gmail.com (i.e. TARGET ACCOUNT 2) to place the transaction and order the flowers to be delivered to the VICTIM in this case. Additionally, AKHTAR listed his phone number as, 804-986-1201. I believe AKHTAR's use of the TARGET ACCOUNT 2 to place the order is significant because it shows use of this Google account in connection with the suspected stalking. Further, I know that individuals placing online orders often receive confirmation messages to the provided email address. As such, I believe TARGET ACCOUNT 2 likely contains information related to this order, as well as other pertinent information.

53. In this case, there are numerous reasons why a search of the TARGET ACCOUNTS is likely to yield evidence of stalking. For example, Google account data for the TARGET ACCOUNTS suspected to be used by AKHTAR is likely to reveal credit card information, which could further confirm his ordering of the flowers. It is likely to yield historical information about AKHTAR's travel to the USAO, VICTIM's residence, or other physical locations potentially significant to VICTIM's frequent locations.

54. Furthermore, Google services are likely to show USMS investigators, past visits to VICTIM's address, searches for news articles about the VICTIM, saved photographs or other data about VICTIM, draft emails composed to or about VICTIM, etc. Training and experience has shown USMS investigators that stalkers will often collect information about someone, including information about their victim's work, family, and other personal information. Further, stalks can even collect images/videos of individuals resembling that person as part of their fascination.

55. As part of this investigation, the USMS obtained a federal warrant to install a GPS tracker and monitor the location of a vehicle used by AKTHAR. During the time period that the vehicle GPS tracker was installed on AKTAR's vehicle (i.e. November 19, 2021 to December 29, 2021), the tracker did not reveal that AKTHAR traveled to VICTIM's residence. Despite the identified use of travel via the vehicle, I believe AKTHAR could still be continuing to stalk the victim via online methods, including use of AKHTAR's Google accounts. Based on my participation in this investigation, as well as my training and experience, I believe it is likely AKTAR has used the internet, including Google services, to locate and find information about VICTIM.

56. In short, I believe that is probable cause to conclude that information pertinent to the crime under investigation will likely be found within the TARGET ACCOUNTS.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

57. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VII. CONCLUSION

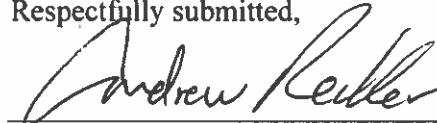
58. Based on the facts set forth above, I submit that probable cause exists to believe the user of the TARGET ACCOUNTS (Google email accounts M.atif.akhtar@gmail.com and akhtarma@gmail.com) has violated 18 U.S.C. § 2261A(2)(B) (Stalking), and that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within the information associated with these Google, LLC accounts for information generated between April 1, 2019 and present.

VIII. REQUEST FOR SEALING & NON-NOTIFICATION

59. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for a period of one year. These documents discuss an ongoing criminal investigation that is not fully known in its details to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

60. Your affiant further requests that, pursuant to 18 U.S.C. § 2705(b), the Court direct that Google, LLC shall not notify any person, including the subscriber of the specified account, of the existence of the warrant, this affidavit, attachments, applications, any returns, and associated paperwork for a period of one-year, because there is reason to believe that any such notification will result in: (1) destruction of or tampering with evidence; (2) intimidation of potential witnesses; and (3) otherwise seriously jeopardize the ongoing investigation by, for example, causing others with knowledge of the suspect's activities to flee or to mask their identity.

Respectfully submitted,



ANDREW RECKER
Deputy United States Marshal
United States Marshals Service

Received by reliable electronic means and sworn to before me
over the telephone and signed by me pursuant to Fed.R.Crim.P. 4.1
on this 15th day of February 2022.

/s/ MRC

HONORABLE MARK R. COLOMBELL
United States Magistrate Judge

Seen and approved:



KATIE BURROUGHS MEDEARIS
Special Assistant United States Attorney

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information, wherever stored, associated with email account M.atif.akhtar@gmail.com (**TARGET ACCOUNT 1**) that is or was stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information, wherever stored, associated with email account akhtarma@gmail.com (**TARGET ACCOUNT 2**) that is or was stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held, or maintained inside or outside the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from the time period of April 1, 2019 to present:

- a. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity from inception to present including account sign in locations, browser information, platform information, account status, and internet protocol (IP) addresses;
- b. Cellular Phone Information - Device make, model, International Mobile Equipment Identifier (IMEI) and a list of installed applications for all associated devices linked to the Google accounts of the target account(s);
- c. Evidence of user attribution - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

- d. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from inception to present, calendar entries, notes, alerts, invites, and invitees;
- e. Contacts - All contacts stored by the Provider including name, all contact phone numbers, emails, social network links, and images;
- f. Documents – All user created documents stored by the Provider;
- g. Email - All email messages from inception to present, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;
- h. Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;
- i. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from inception to present;

- j. Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;
- k. Search History - All search history and queries from inception to present, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;
- l. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device from inception to present;
- m. Wallet/Checkout - All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book from inception to present;
- n. Google Drive – All live and deleted files stored in the listed user's Google Drive;
- o. Google Hangouts – All messages from inception to present, including by way of example and not limitation, such as messages whether read or unread, sent messages, saved drafts, chat histories, and deleted messages. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, the message content, and all attached files;
- p. A list of linked accounts based upon IP address and session cookie;
- q. The types of services utilized;

- r. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and
- s. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2261A(2)(B), (Stalking) and involve M.atif.akhtar@gmail.com and akhtarma@gmail.com as described in Attachments A-1 and A-2, including information pertaining to the following matters:

- a. Communications between AKTHAR and any other parties, or saved draft communications, Google searches, photographs, calendar entries, or other documents relating to VICTIM, including but not limited to information about:
 - a. VICTIM's birthday;
 - b. VICTIM's career, including any cases under investigation by the U.S. Attorney's Office (USAO) in the Eastern District of Virginia (EDVA);
 - c. VICTIM's vehicle;
 - d. phone numbers, fax numbers, or addresses for the USAO EDVA or federal courthouses within the EDVA;
 - e. VICTIM's location(s), such as his/her work address, current home address, or prior residences;

- f. VICTIM's family members or close associates;
 - g. flower delivery services;
 - h. the purchase, sale, possession, or research about firearms or ammunition;
 - i. security protocols employed by DOJ or USMS;
 - j. collection of images, videos, or other content of individuals resembling VICTIM and/or about "Barbie" or "Ken";
 - k. threats or acts of violence; or
 - l. or other data involved in the crime of stalking under investigation.
- b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- c. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- d. Evidence indicating the account owner's state of mind as it relates to the crime under investigation, including evidence of paranoia and/or obsessive conduct;
- e. Evidence related to the user's travel to areas frequented by the VICTIM, such as any EDVA USAO or federal courthouse in EDVA;
- f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- g. The identity of the person(s) who communicated with the user ID about matters relating to the crime under investigation, including records that help reveal their whereabouts;
- h. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC, and they were made by Google, LLC as a regular practice; and

b. such records were generated by Google, LLC electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature